ORIGINAL

MICHAEL M. CARLSON (Bar No. 88048)
BRYAN J. WILSON (Bar No. 138842)
JANA G. GOLD (Bar No. 154246)
Morrison & Foerster
755 Page Mill Road
Palo Alto, California 94304-1018
Telephone: (415) 813-5600
Facsimile: (415) 494-0792

PATRICK J. FLINN (Bar No. 104423)
ALSTON & BIRD
One Atlantic Center
1201 West Peachtree Street
Atlanta, Georgia 30309
Telephone: (404) 881-7000
Facsimile: (404) 881-8777

Attorneys for Proposed Intervenor
CARO-KANN CORPORATION

FILED
Nov 1 3 31 PM '95
RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA. S.J.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROGER SCHLAFLY,

Plaintiff,

v.

PUBLIC KEY PARTNERS and RSA DATA SECURITY, INC.,

Defendants.

No. CV 94 20512 SW

REPLY DECLARATION OF JANA GOLD IN SUPPORT OF CKC'S MOTION TO INTERVENE PURSUANT TO FRCP 24(a)

Date: November 15, 1995
Time: 10:00 a.m.
Courtroom: 14

I, Jana Gold, declare:

1. I am an attorney with the law firm of Morrison & Foerster, attorneys of record for proposed intervenor Caro-Kann Corporation. I make this declaration based on personal knowledge, unless otherwise stated, and if called as a witness I could and would testify competently thereto.

2. Attached to this declaration as Exhibit 1 is a true and correct copy of a document clarifying the assignment of rights to sue on the Stanford patents as between Cylink Corporation and Caro-Kann Corporation ("CKC").

3. Attached to this declaration as Exhibit 2 is a true and correct copy of PKP's responses to Plaintiff's Requests for Admission in this case, served on October 23, 1995. Counsel for CKC did not participate in drafting these responses and did not have an opportunity to review them before they were served. I have been informed that CKC's president Robert Fougner did not participate in drafting PKP's responses either.

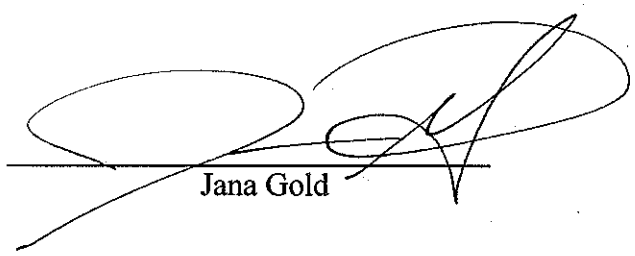
4. Attached to this declaration as Exhibit 3 is a true and correct copy of a document entitled "Information on Cylink's License Package" which was printed out by this office from RSADSI's Home Page on the World Wide Web.

5. CKC moved to intervene in this case as soon as possible after the arbitrator's decision was released, and noticed the motion for the first available date under the applicable rules of procedure. When Mr. Schlafly informed CKC of a scheduling conflict on that date, CKC agreed to move the hearing to an earlier date, but explained to Mr. Schlafly that it could not agree to reschedule the motion for a later date because CKC did not want to delay upcoming dates for summary judgment motions and other pre-trial and trial related dates.

6. CKC does not intend to take any discovery in this action beyond the discovery that has already been initiated by the current parties. CKC's counsel represented the inventors of the Stanford patents in recent depositions taken by Mr. Schlafly. CKC does intend to participate in ongoing discovery and any additional discovery that may be propounded by the current parties.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed this 1st day of November, 1995 in Palo Alto, California.



Jana Gold

1

# ASSIGNMENT OF RIGHTS

This Agreement is entered into as of September 6, 1995, (the "Effective Date") by and between Cylink Corporation, a California Corporation having its principal place of business at 910 Hermosa Court, Sunnyvale, CA 94086 ("Cylink") and its wholly owned subsidiary, Caro-Kann Corporation, a California corporation having its principal place of business at 910 Hermosa Court, Sunnyvale, CA 94086 ("CKC").

WHEREAS, on August 25, 1989, The Board of Trustees of the Leland Stanford Junior University ("Stanford") granted Cylink an exclusive license (the Stanford License"), including the rights to institute actions against third parties for infringement and grant sublicenses, to the following U.S. Patents and their foreign equivalents (collectively, the "Patents):

**Cryptographic Apparatus and Method ("Hellman-Diffie")..... No. 4,200,770**

**Public Key Cryptographic Apparatus and Method ("Hellman-Merkle")..... No. 4,218,582**

**Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig")..... No. 4,424,414**

WHEREAS, on April 6, 1990, Stanford and Cylink agreed to amend Cylink's license and transfer certain of Cylink's rights, including the right to institute actions for infringement and to grant sublicenses to the Patents, to Public Key Partners, a California general partnership ("PKP") between CKC and RSA Data Security, Inc.;

WHEREAS, on September 6, 1995, a panel of duly appointed arbitrators issued their Decision and Order dissolving PKP;

WHEREAS, pursuant to the terms of the Stanford License, as amended, CKC now holds exclusive sublicensing rights to the Patents;

WHEREAS, CKC is currently in the business of sublicensing the Patents and is actively promoting licensing of the Patents to third parties;

WHEREAS, as between CKC and Cylink, it is CKC which has the responsibility for resolving claims for infringement of the Patents by third parties;

Assignment of Rights
Concerning Infringement
of Stanford Patents
Cylink and CKC

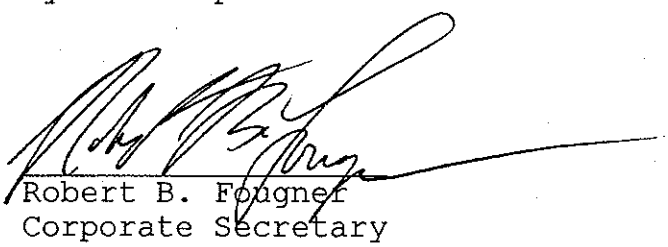
AND WHEREAS, Cylink and CKC wish to eliminate any ambiguity, to the extent that any ambiguity may exist, that CKC has the right as well as the responsibility for pursuing claims for infringement of the Patents by third parties;

NOW THEREFORE, it is hereby agreed, as follows:

1. All right, title and interest of Cylink to claims against third parties for infringement of the Patents, including the right to institute and prosecute actions against any such third parties for infringement, are hereby transferred and assigned to CKC, to the extent such rights are not already assigned to CKC.

2. All other rights of Cylink under the Stanford License shall remain in full force and effect.

Cylink Corporation



Robert B. Fougner
Corporate Secretary

2

RECD SEP 7 1995

CALENDARED

Roger Schlafly, Pro Se
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

In the United States District Court
for the Northern District of California

| | |
|---|---|
| ROGER SCHLAFLY, Plaintiff | ) Case C-94-20512 SW PVT |
| v. | ) First Plaintiff Request for Admission of Facts |
| PUBLIC KEY PARTNERS, and RSA DATA SECURITY INC., Defendants. | ) Sept. 5, 1995 |

First Plaintiff Request for Admission of Facts. Defendants PKP and RSADSI are requested to respond pursuant to FRCP Rule 36.

Please admit the following as facts. Refer to Amended Complaint and the Plaintiff's Motion for Partial Summary Judgment for definitions.

1. Exhibits A to Z, AA to AH of the Amended Complaint are all authentic.

2. Exhibits CA to CI of the Plaintiff's Motion for Partial Summary Judgment are all authentic.

3. Each reference to "Diffie" in the above exhibits is to the same person. Likewise with Rivest, Hellman, Merkle, Adleman, Shamir, Bidzos, Fougner, Schlafly, and Schnorr.

4. Each and every allegation in the Amended Complaint.

5. Exhibit CA is a copy of a document which was publicly distributed in August 1976.

6. Exhibit CA is a full disclosure of the Diffie-Hellman invention.

7. Exhibit CA is a preprint of Exhibit U.

8. The Diffie-Hellman invention was disclosed to the public in a lecture by Diffie in June 1976.

9. The Diffie-Hellman invention was disclosed to the public in a lecture by Hellman in June 1976.

Case 5:94-cv-20512-SW Document 98 Filed 11/01/95 Page 9 of 30

10. The fundamental ideas of public key cryptography are disclosed in Exhibit T.

11. The Diffie-Hellman patent does not disclose or claim a public key cryptosystem.

12. The account given in Exhibit V of the breaking of the trapdoor knapsack is accurate.

13. The trapdoor knapsack described in Exhibit V is the same invention as that disclosed in the Hellman-Merkle patent.

14. Merkle paid off bets of $100 and $1000 when the Hellman-Merkle invention was shown to not meet its stated objectives.

15. The $1000 offered in Exhibit CC was paid to Ernie Brickell in or around 1985.

16. The Hellman-Merkle patent disclosure does not enable someone skilled in the art (up to 1978) to make a secure cryptosystem.

17. As a matter of law, a Hellman-Merkle patent claim is invalid unless it is realized by at least one of its disclosed embodiments.

18. The only two embodiments of a cryptosystem disclosed in Hellman-Merkle are what is commonly called the "trapdoor knapsack" and the "multiple iteration knapsack".

19. None of the embodiments disclosed in Hellman-Merkle achieve any of the objects of the invention stated in col. 2 of the patent.

20. The methods of claims 4 and 5 of Hellman-Merkle are not shown in any of the patent diagrams.

21. The method of claims 4 of Hellman-Merkle is a method for what is commonly called "digital signature with message recovery".

22. No practical method for digital signatures is disclosed in Hellman-Merkle.

23. The computational infeasibility of Hellman-Merkle patent claims 1-6 and 14-17 is not achieved by any of the disclosed embodiments, where "computationally infeasible" is defined as in Exhibit T or as in col. 5, lines 10-14, of the Hellman-Merkle patent.

24. There is a consensus in the cryptographic community that the Hellman-Merkle invention is useless.

25. The Hellman-Merkle invention is useless.

26. PKP partners RSADSI and Cylink have known the Hellman-Merkle invention to be worthless since at least 1985, and have not used it in their commercial products.

27. The Hellman-Merkle invention is fully disclosed in Exhibit CE.

28. Exhibit CB is an accurate account of the failure of the Hellman-Merkle invention.

29. The Hellman-Merkle patent does not disclose a method of digital signature generation or verification which avoids message encryption.

30. Practice of the DSA does not infringe the Schnorr patent.

31. The "rejuvenation" scheme of Schnorr, specified in col. 9-10 and claim 5 of the Schnorr patent, has been broken and does not achieve the claimed security. In particular, it does not achieve the object of the invention stated in col. 2, line 25-30.

32. Claim 5 of the Schnorr patent is invalid and unenforceable.

33. Exhibit CD is a full disclosure of the RSA invention.

34. The practice of the RSA invention is enabled by Exhibit U, section V of Exhibit CD, and standard computer science textbooks available in 1977.

35. The RSA invention is fully disclosed in Exhibit CE.

36. The RSA invention is fully disclosed in Exhibit CF.

37. The RSA invention is fully disclosed in Exhibit CI.

38. RSADSI regards any cryptographic applications of the formula

$$Y = X^e \bmod N,$$

where N is a large composite number, to be an infringement of the RSA patent.

39. There is a four-line Perl script which RSADSI regards as an infringement of the RSA patent.

40. PKP never offered ISC a patent license.

41. PKP has never complied with the IEEE patent policy.

42. PKP led ANSI to believe it would comply with the ANSI patent policy when ANSI drafted its X9.31 proposed standard for RSA signatures.

43. PKP has refused to give ANSI the assurances necessary for ANSI to adopt X9.31 as a standard.

44. The federal Digital Signature Standard was delayed at least a year by PKP asserting patent claims against the DSA.

45. Fougner has asserted that the US Government may not practice the DSA without obtaining a license to the Schnorr patent.

46. Bidzos has threatened lawsuits against users of the DSA who fail to license PKP patents.

47. The best mode disclosed in the Diffie-Hellman patent is what is popularly called the single iteration trapdoor knapsack.

48. The RSA patent does not disclose any novel hardware.

49. The RSA invention is fully disclosed in Exhibit CI.

50. A public key cryptosystem is not secure if it is feasible for an adversary to compute the private key from the corresponding public key.

Dated: Sept 5, 1995

By: _____

Plaintiff, Roger Schlafly, Pro Se

Thomas R. Hogan, Esq., California State Bar No. 042048
John P. Shinn, Esq., California State Bar No. 175598
LAW OFFICES OF THOMAS R. HOGAN
60 South Market Street, Suite 1125
San Jose, CA 95113-2332
Telephone: (408) 292-7600

Attorneys for Defendant
PUBLIC KEY PARTNERS

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| ROGER SCHLAFLY,<br><br>Plaintiff,<br><br>v.<br><br>PUBLIC KEY PARTNERS and RSA DATA SECURITY, INC.,<br><br>Defendants. | No. CV 94 20512 SW (PVT)<br><br>DEFENDANT PUBLIC KEY PARTNERS' RESPONSES TO FIRST PLAINTIFF REQUEST FOR ADMISSION OF FACTS |

PROPOUNDING PARTY: Plaintiff, ROGER SCHLAFLY

RESPONDING PARTY: Defendant, PUBLIC KEY PARTNERS

SET NUMBER: One

Pursuant to Federal Rule of Civil Procedure, defendant PUBLIC KEY PARTNERS, does hereby respond to the Request for Admissions served by plaintiff, above-named, as follows:

REQUEST FOR ADMISSION NO. 1

Exhibits A to Z, AA to AH of the Amended Complaint are all authentic.

////

**RESPONSE TO REQUEST FOR ADMISSION NO. 1**

Objection: PKP objects to this request on the grounds that it is vague, ambiguous and unintelligible in that PKP has to speculate as to the meaning of the word "authentic" as used in this request.

Defendant Public Key Partners cannot truthfully admit or deny this allegation for the reason that although defendants have made reasonable inquiry, defendants have been unable to locate the source of or verify the authenticity of said documents and, therefore, the information known to them is insufficient to admit or deny the same.

**REQUEST FOR ADMISSION NO. 2**

Exhibits CA to CI of the Plaintiff's Motion for Partial Summary Judgment are all authentic.

**RESPONSE TO REQUEST FOR ADMISSION NO. 2**

Objection: PKP objects to this request on the grounds that it is vague, ambiguous and unintelligible in that PKP has to speculate as to the meaning of the word "authentic" as used in this request.

Defendant Public Key Partners cannot truthfully admit or deny this allegation for the reason that although defendants have made reasonable inquiry, defendants have been unable to locate the source of or verify the authenticity of said documents and, therefore, the information known to them is insufficient to admit or deny the same.

/ / / /

/ / / /

/ / / /

**REQUEST FOR ADMISSION NO. 3**

Each reference to "Diffie" in the above exhibits is to the same person. Likewise with Rivest, Hellman, Merkle, Adleman, Shamir, Bidzos, Fougner, Schlafly, and Schnorr.

**RESPONSE TO REQUEST NO. 3**

Defendant Public Key Partners cannot truthfully admit or deny this allegation for the reason that although defendants have made reasonable inquiry, defendants have been unable to locate the source of or verify the accuracy of said documents and, therefore, the information known to them is insufficient to admit or deny the same.

**REQUEST FOR ADMISSION NO. 4**

Each and every allegation in the Amended Complaint.

**RESPONSE TO REQUEST FOR ADMISSION NO. 4**

PKP incorporates herein by reference each and every admission, denial and denial on information and belief that it stated in its Answer to the Amended Complaint.

**REQUEST FOR ADMISSION NO. 5**

Exhibit CA is a copy of a document which was publicly distributed in August 1976.

**RESPONSE TO REQUEST FOR ADMISSION NO. 5**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 6**

Exhibit CA is a full disclosure of the Diffie-Hellman invention.

**RESPONSE TO REQUEST FOR ADMISSION NO. 6**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 7**

Exhibit CA is a preprint of Exhibit U.

**RESPONSE TO REQUEST FOR ADMISSION NO. 7**

PKP cannot truthfully admit or deny this allegation for the reason that although defendants have made reasonable inquiry, defendants have been unable to locate the source of or verify the accuracy of said documents and, therefore, the information known to them is insufficient to admit or deny the same.

**REQUEST FOR ADMISSION NO. 8**

The Diffie-Hellman invention was disclosed to the public in a lecture by Diffie in June 1976.

**RESPONSE TO REQUEST FOR ADMISSION NO. 8**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 9**

The Diffie-Hellman invention was disclosed to the public in a lecture by Hellman in June 1976.

**RESPONSE TO REQUEST FOR ADMISSION NO. 9**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 10**

The fundamental ideas of public key cryptography are disclosed in Exhibit T.

**RESPONSE TO REQUEST FOR ADMISSION NO. 10**

Objection: PKP objects to this request on the grounds that it is vague, ambiguous and unintelligible in that PKP has to speculate as to the meaning of the word "fundamental" as used in this request. Without waiving this objection, PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 11**

The Diffie-Hellman patent does not disclose or claim a public key cryptosystem.

**RESPONSE TO REQUEST FOR ADMISSION NO. 11**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 12**

The account given in Exhibit V of the breaking of the trapdoor knapsack is accurate.

**RESPONSE TO REQUEST FOR ADMISSION NO. 12**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 13**

The trapdoor knapsack described in Exhibit V is the same invention as that disclosed in the Hellman-Merkle patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 13**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 14**

Merkle paid off bets of $100 and $1000 when the Hellman-Merkle invention was shown to not meet its stated objectives.

**RESPONSE TO REQUEST FOR ADMISSION NO. 14**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 15**

The $1000 offered in Exhibit CC was paid to Ernie Brickell in or around 1985.

**RESPONSE TO REQUEST FOR ADMISSION NO. 15**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 16**

The Hellman-Merkle patent disclosure does not enable someone skilled in the art (up to 1978) to make a secure cryptosystem.

**RESPONSE TO REQUEST FOR ADMISSION NO. 16**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 17**

As a matter of law, a Hellman-Merkle patent claim is invalid unless it is realized by at least one of its disclosed embodiments.

**RESPONSE TO REQUEST FOR ADMISSION NO. 17**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 18**

The only two embodiments of a cryptosystem disclosed in Hellman-Merkle are what is commonly called the "trapdoor knapsack" and the "multiple iteration knapsack".

**RESPONSE TO REQUEST FOR ADMISSION NO. 18**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 19**

None of the embodiments disclosed in Hellman-Merkle achieve any of the objects of the invention stated in col. 2 of the patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 19**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 20**

The methods of claims 4 and 5 of Hellman-Merkle are not shown in any of the patent diagrams.

**RESPONSE TO REQUEST FOR ADMISSION NO. 20**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 21**

The method of claims 4 of Hellman-Merkle is a method for what is commonly called "digital signature with message recovery".

**RESPONSE TO REQUEST FOR ADMISSION NO. 21**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 22**

No practical method for digital signatures is disclosed in Hellman-Merkle.

**RESPONSE TO REQUEST FOR ADMISSION NO. 22**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 23**

The computational infeasibility of Hellman-Merkle patent claims 1-6 and 14-17 is not achieved by any of the disclosed embodiments, where "computationally infeasible" is defined as in Exhibit T or as in col. 5, lines 10-14, of the Hellman-Merkle patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 23**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 24**

There is a consensus in the cryptographic community that the Hellman-Merkle invention is useless.

**RESPONSE TO REQUEST FOR ADMISSION NO. 24**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 25**

The Hellman-Merkle invention is useless.

**RESPONSE TO REQUEST FOR ADMISSION NO. 25**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 26**

PKP partners RSADSI and Cylink have known the Hellman-Merkle invention to be worthless since at least 1985, and have not used it in their commercial products.

**RESPONSE TO REQUEST FOR ADMISSION NO. 26**

PKP objects to this Request on the ground that this Request is properly directed to non-party Caro-Kann Corporation and/or RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 27**

The Hellman-Merkle invention is fully disclosed in Exhibit CE.

**RESPONSE TO REQUEST FOR ADMISSION NO. 27**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 28**

Exhibit CB is an accurate account of the failure of the Hellman-Merkle invention.

**RESPONSE TO REQUEST FOR ADMISSION NO. 28**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 29**

The Hellman-Merkle patent does not disclose a method of digital signature generation or verification which avoids message encryption.

**RESPONSE TO REQUEST FOR ADMISSION NO. 29**

PKP lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 30**

Practice of the DSA does not infringe the Schnorr patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 30**

PKP denies this Request.

**REQUEST FOR ADMISSION NO. 31**

The "rejuvenation" scheme Schnorr, specified in col. 9-10 and claim 5 of the Schnorr patent, has been broken and does not achieve the claimed security. In particular, it does not achieve the object of the invention stated in col. 2, line 25-30.

**RESPONSE TO REQUEST FOR ADMISSION NO. 31**

PKP objects to this Request on the grounds that it is irrelevant and not calculated to lead to the discovery of admissible evidence. Without waiving this objection, PKP responds that it lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 32**

Claim 5 of the Schnorr patent is invalid and unenforceable.

**RESPONSE TO REQUEST FOR ADMISSION NO. 32**

PKP objects to this Request on the grounds that it is irrelevant and not calculated to lead to the discovery of admissible evidence. Without waiving this objection, PKP responds that it lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 33**

Exhibit CD is a full disclosure of the RSA invention.

**RESPONSE TO REQUEST FOR ADMISSION NO. 33**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 34**

The practice of the RSA invention is enabled by Exhibit U, section V of Exhibit CD, and standard computer science textbooks available in 1977.

**RESPONSE TO REQUEST FOR ADMISSION NO. 34**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 35**

The RSA invention is fully disclosed in Exhibit CE.

**RESPONSE TO REQUEST FOR ADMISSION NO. 35**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 36**

The RSA invention is fully disclosed in Exhibit CF.

**RESPONSE TO REQUEST FOR ADMISSION NO. 36**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 37**

The RSA invention is fully disclosed in Exhibit CI.

**RESPONSE TO REQUEST FOR ADMISSION NO. 37**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 38**

RSADSI regards any cryptographic applications of the formula

$$Y = X^e \bmod N,$$

where N is a large composite number, to be an infringement of the RSA patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 38**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 39**

There is a four-line Perl script which RSADSI regards as an infringement of the RSA patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 39**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 40**

PKP never offered ISC a patent license.

**RESPONSE TO REQUEST FOR ADMISSION NO. 40**

Denied.

**REQUEST FOR ADMISSION NO. 41**

PKP has never complied with the IEEE patent policy.

**RESPONSE TO REQUEST FOR ADMISSION NO. 41**

Denied.

**REQUEST FOR ADMISSION NO. 42**

PKP led ANSI to believe it would comply with the ANSI patent policy when ANSI drafted its X9.31 proposed standard for RSA signatures.

**RESPONSE TO REQUEST FOR ADMISSION NO. 42**

PKP denies any negative connotation associated with plaintiff's use of the phrase "PKP led ANSI to believe." Except as expressly denied, PKP admits this Request.

**REQUEST FOR ADMISSION NO. 43**

PKP has refused to give ANSI the assurances necessary for ANSI to adopt X9.31 as a standard.

**RESPONSE TO REQUEST FOR ADMISSION NO. 43**

Denied.

**REQUEST FOR ADMISSION NO. 44**

The federal Digital Signature Standard was delayed at least a year by PKP asserting patent claims against the DSA.

**RESPONSE TO REQUEST FOR ADMISSION NO. 44**

PKP lacks sufficient information and belief on which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 45**

Fougner has asserted that the US Government may not practice the DSA without obtaining a license to the Schnorr patent.

**RESPONSE TO REQUEST FOR ADMISSION NO. 45**

PKP admits this Request.

**REQUEST FOR ADMISSION NO. 46**

Bidzos has threatened lawsuits against users of the DSA who fail to license PKP patents.

**RESPONSE TO REQUEST FOR ADMISSION NO. 46**

PKP denies this Request.

**REQUEST FOR ADMISSION NO. 47**

The best mode disclosed in the Diffie-Hellman patent is what is popularly called the single iteration trapdoor knapsack.

**RESPONSE TO REQUEST FOR ADMISSION NO. 47**

PKP responds that it lacks sufficient information and belief with which to admit or deny this Request, and, on that basis, denies this Request.

**REQUEST FOR ADMISSION NO. 48**

The RSA patent does not disclose any novel hardware.

**RESPONSE TO REQUEST FOR ADMISSION NO. 48**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 49**

The RSA invention is fully disclosed in Exhibit CI.

**RESPONSE TO REQUEST FOR ADMISSION NO. 49**

PKP objects to this Request on the ground that this Request is properly directed to defendant RSADSI, who has more information on which to base an admission or denial to this request.

**REQUEST FOR ADMISSION NO. 50**

A public key cryptosystem is not secure if it is feasible for an adversary to compute the private key from the corresponding public key.

**RESPONSE TO REQUEST FOR ADMISSION NO. 50**

PKP admits this Request.

Dated: 10/23/95

THOMAS R. HOGAN
JOHN P. SHINN

Attorneys for Defendant
PUBLIC KEY PARTNERS

3

# Information on Cylink's "License Package"

## TO: All Current and Potential RSA Software Customers

RSA has been informed that some of our licensees have received a "license package" from Robert Fougner at Cylink, offering to license the so-called Stanford Patents, and threatening legal reprisals to those who do not. The package contains serious inaccuracies that are clearly self-serving and constructed to coerce the recipient into an unnecessary license.

We would advise everyone to remember to always take Cylink's statements with a rather large grain of salt. We realize that the Cylink package is frightening, and we are saddened to see that, in their frustration in their inability to successfully attack RSA, Cylink's venom for us has been directed against our customers.

RSA specific recommendation/policy respecting the Cylink package is as follows:

1. It is RSA's position that our licensees **do not need** a Stanford Patent license from Cylink in order to use the software licensed by RSA, as long as the RSA licensee complies with the terms of their RSA license.

2. The final decision to license the Stanford Patents is up to the individual RSA customer, though we strongly recommend that they not do so. Contrary to implications made by Cylink in their license package, RSA will not reimburse licensees for any sums paid to Cylink for a Stanford Patent license. We feel that Cylink is attempting to coerce our customers into buying an expensive license that is not necessary.

3. If Cylink ever backs up its threats and actually sues any RSA licensee based on infringement of the Stanford Patents, we will stand behind the indemnity provisions of our license agreements and vigorously defend our customers, at our expense.

In fact, we've already taken steps to protect our licensees by filing a lawsuit in Federal Court specifically seeking a declaration that a Stanford Patent license is not necessary for the use of RSA's software.

Our final word is this: RSA will continue to take whatever steps are necessary to protect our licensees.

If you have any questions or comments, please do not hesitate to contact Paul Livesay, RSA's Director of Legal Affairs, at 415/595-8782.

[ **RSA Home** | **What's New** ]

**Copyright © 1995 RSA Data Security, Inc. All rights reserved.**
**10/17/95**



EXHIBIT 3